Prepare For Minn. Privacy Law To Catch Up To Calif., Wash.

By **Michael Reif and Akina Khan** (April 2, 2021)

Michael Reif

Akina Khan

Minnesota is the latest state to tackle the thorny issues of data privacy, and the nascent 2021 legislative session has already seen the introduction of two competing measures aimed at expanding data privacy protections.

Each bill takes strong cues from privacy legislation in other states — the California Consumer Privacy Act and the proposed Washington Privacy Act — setting up what is emerging as a two-track approach to state-focused privacy regulation in the U.S.

California, as the pioneer in privacy regulation among the states, went beyond the data breach focus of existing state privacy laws with the CCPA and allowed consumers to opt out of sales of their personal information, make data access requests, and receive increased guidance about their privacy rights in companies' privacy policies.

On the heels of the CCPA's passage and with prodding from Microsoft Corp., legislators in Washington introduced the WPA, adding, among others, a right to correction, which was not originally in the CCPA, though recently added with the passage of the California Privacy Rights Act.

The WPA, however, lacks a private right of action and entrusts all enforcement to the Washington state attorney general. After failing to become law in 2019 and 2020, a new draft of the WPA, featuring added measures that address the processing of personal information for public health emergencies, including contact tracing, has been introduced in the state Legislature.

Recently, following the WPA framework, Virginia became the second state to enact comprehensive privacy protections for consumers.[1]

In Minnesota, after two years in which WPA-like proposals failed to become law, the first data privacy bill of the 2021 session — H.F. 36 — changed course and took a CCPA approach. Weeks later, with H.F. 1492, a WPA-like bill reemerged.

Though divergent in some protections and enforcement mechanisms, as discussed below, both bills would substantially alter the privacy landscape in Minnesota and require additional efforts from businesses handling the personal information of Minnesota citizens.

Minnesota H.F. 36 — A CCPA-Style Data Privacy Act With Teeth

With the introduction of H.F. 36 on Jan. 7, Democratic Rep. Mohamud Noor appeared to shift the trend in Minnesota from the trending WPA approach back to the CCPA.[2] His bill gives various rights to consumers to protect and control their personal data and is enforceable by the state attorney general.[3]

The obligations imposed by the bill apply to any for-profit entity that:

- Has annual gross revenues in excess of $25 million;

- Annually buys or sells the personal information of 50,000 or more consumers, households or devices; or

- Derives 50% or more of the business's annual revenues from selling consumers' personal information.[4]

Like the CCPA, the bill also applies extraterritorially and covers businesses that share common branding and control with a separate business that meets the three criteria.[5]

The bill gives consumers the right to access[6] and delete[7] their personal information, opt out of the sale of their personal information,[8] and not be discriminated against for exercising such rights.[9] However, under certain circumstances, businesses may retain consumer information despite a request for deletion.[10]

As under the CCPA, H.F. 36 would require businesses to notify consumers of the businesses' data collection and disclosure practices[11] and provide consumers two or more designated methods for opting out of information sales.[12]

Perhaps most notably, H.F. 36 expands upon the CCPA's enforcement model by granting consumers a private right of action with statutory damages of $100 to $750, per consumer, per incident, or the amount of actual damages, whichever is greater.[13]

Under that provision, consumers could sue over any violation of the act — not just in the event of a data breach, as in California. H.F. 36's combination of a broad private right of action and statutory damages would make it instantly the most aggressive data privacy law in the U.S. if passed.

Minnesota H.F. 1492: A WPA-Like Approach

Privacy rights activists and the plaintiffs bar excited about that potential enforcement mechanism should keep their enthusiasm at bay, however, because just one month after the introduction of H.F. 36, Democratic Rep. Steve Elkins resurrected the WPA-like legislation he introduced in 2019 and 2020 with H.F. 1492, the proposed Minnesota Consumer Data Privacy Act, or MCDPA.

Like its WPA counterpart, the MCDPA includes the rights to confirm, correct, delete, access and opt out of personal data being processed and sold by covered businesses.[14]

Unlike H.F. 36, the proposed MCDPA is limited to Minnesota consumers and applies only to businesses that target or conduct business in Minnesota.[15] The act defines personal information more narrowly by expressly excluding deidentified and public data from the scope of protected information.[16]

Similarly, the definition of consumer in the MCDPA is narrower, as it excludes employees of the business.[17] H.F. 36 defines consumer as any natural person.[18]

The MCDPA would also grant consumers the additional right to correct their information[19]

and eliminates the business purpose exception from H.F. 36 that excuses businesses from complying with consumer requests under enumerated circumstances.[20] Elkins' 2020 bill had similarly excluded the business purpose loopholes due to his concerns following consultation with privacy groups.[21]

Perhaps the starkest difference between the two 2021 bills is their approach to enforcement. While H.F. 36 provides for a private right of action,[22] the proposed MCDPA relies entirely on the office of the attorney general for enforcement of both breach-related harm and of MCDPA violations.[23] This attorney general-centric approach adds the weight of the state to MCDPA enforcement, but in practice, it has the potential to water down the act's effectiveness.

In California, for example, when the CCPA charged the attorney general with all nonbreach enforcement, that underresourced office found itself unable to initiate more than a handful of CCPA-related enforcement actions per year. That untenable situation was a driving force behind Californians' voting to create a stand-alone Data Privacy Protection Agency as part of the recently passed California Privacy Rights Act.

What's Next for Data Privacy in Minnesota?

Since their introduction, both H.F. 36 and H.F. 1492 have been referred to the House's Commerce, Finance and Policy Committee for further discussion. Though each remains technically viable, the MCDPA, with its attorney general-only enforcement mechanism, appears more likely to gain traction.

Unlike H.F. 36, the Elkins bill has a companion bill working its way through the Minnesota Senate. And, interestingly, H.F. 36 author Noor has signed on as a co-sponsor of H.F. 1492 — a tacit endorsement of the WPA approach that the MDCPA proposes.

Minnesotans will know more about the fate of the MDCPA in the coming weeks, as the Legislature kicks into high gear in anticipation of the May 17 adjournment date for its regular session.

What Can Businesses Do to Prepare?

Although nonprofit corporations will not have to comply with the MCDPA until July 31, 2026, if passed, the MCDPA would become effective as of July 31, 2022, for all covered businesses.[24] To avoid costly fines and lawsuits from noncompliance or a rushed approach to compliance, businesses would be wise to start preparing now.

The first step that businesses can take immediately is to track the developments of the MCDPA, as amendments related to enforcement are likely. Targeted lobbying and industry-based impact analysis for legislators could play an important role in shaping the ultimate form of the bill.

Now is also a prudent time for businesses to start — if they haven't already — conversations with their compliance teams.

This is especially true if the business qualifies as a controller rather than a processor. As the ultimate end users of collected information, controllers are subject to greater scrutiny under the MCDPA. The controller is responsible for responding to consumer requests; complying with transparency, nondiscrimination, and use restrictions; and developing guidelines for compliance by the processors.[25]

These obligations are a distinct departure from Minnesota's existing laissez-faire approach to consumer data.

Businesses should give themselves enough time to plan and implement compliance plans because such an overhaul of business protocol often takes more time than anticipated. Strategically planning responses to the eventual enactment of a consumer privacy act in Minnesota can vastly minimize costs in the future.

As important, proper preparation can allow forward-thinking companies to promote their compliance with and commitment to protecting consumer data and privacy — a growing differentiator across all industries.

Michael D. Reif is a partner and Akina R. Khan is an associate at Robins Kaplan LLP.

[1] Rafael Reyneri & Libbie Canter, Virginia Enacts Comprehensive Privacy Law, Inside Privacy (Mar. 4, 2021), https://www.insideprivacy.com/data-privacy/virginia-enacts-comprehensive-privacy-law/.

[2] HF 36, Office of the Revisor of Statutes, https://www.revisor.mn.gov/bills/bill.php?view=chrono&f=HF0036&y=2021&ssn=0&b=house#actions (last visited Feb. 15, 2021).

[3] H.F. 36, 92d Leg., Reg. Sess. (Minn. 2021) [hereinafter HF 36].

[4] HF 36, sec. 2, subd. 1.

[5] Id. para. (b).

[6] Id. sec. 5.

[7] Id. sec. 7, subd. 1.

[8] Id. sec. 6.

[9] Id. sec. 8.

[10] Id. sec. 7, subd. 2.

[11] Id. sec. 3, subd. 1.

[12] Id. subd. 2.

[13] Id. sec. 9, subd. 1.

[14] H.F 1492, 92d Leg., Reg. Sess. (Minn. 2021) [hereinafter HF 1492].

[15] Compare HF 36, sec. 2, subd. 1, with HF 1492, sec. 3, subd. 1.

[16] HF 1492, sec. 2(m).

[17] Id. sec. 3, subd. 2(a)(12).

[18] HF 36, sec. 1, subd. 6.

[19] HF 1492, sec. 5, subd. 1(c).

[20] HF 36, sec. 1, subd. 3.

[21] Issie Lapowsky, Microsoft Can't Get Its Privacy Bill Passed in Its Home State. It's Trying Its Luck Elsewhere, Protocol (Apr. 28, 2020), https://www.protocol.com/microsoft-privacy-bills-in-four-other-states.

[22] HF 36, sec. 9, subd. 1(b).

[23] HF 1492, sec. 10.

[24] HF 1492, sec. 12.

[25] Id. secs. 4, 5, 7.